Section III:	**Application Security**
Title:	**User Authorization and Authentication Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**June 4, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To provide guidance to the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices for establishing standards to prevent unauthorized access to information technology (IT) systems, promote user accountability, and ensure integrity of systems and data.

STANDARD

1.0 Background

User authorization encompasses the protection efforts needed to address the confidentiality, integrity, and authenticity of the organization's data resources. The primary focus of this standard is use of proper access controls. Proper implementation of this standard will grant access to an organization's data resources to only those that need it and prevent unauthorized access.

2.0 Restricting Access

Divisions and Offices shall establish and implement controls appropriate to their line of business to ensure that access to IT systems is on a 'need to know' or 'need to access' basis aligned with job functions. Users shall only be provided access to IT systems in accordance with the NC DHHS Security Standards, Application Security - Application Security Control Standard. Divisions or Offices may change, restrict, or eliminate user access privileges at any time. User access privileges shall be evaluated when a workforce member changes positions to ensure appropriate access is assigned. Upon termination of employment a workforce member's access will be discontinued.

3.0 Managing User Access

Divisions and Offices shall be responsible for establishing a procedure for managing access rights for users of their IT systems and networks throughout the life cycle of the user identification (ID). A request for access to IT systems or applications shall be completed by the user's supervisor and authorized by the business owner of that system. Access requests to IT systems and application resources shall be documented in a standardized format (either in print or electronic) determined by the Division or Office and kept in a secure location. Documentation of access rights shall include the following:

- Information about the user
- The type and duration of access
- Section (work group) information
- Any other necessary information to track the type of access needed for a workforce member

Users will only be granted access to IT systems after undergoing appropriate job or functional training. The user's manager is responsible for ensuring that the user completes the appropriate training for their position before an ID is assigned. All completed training should be documented and kept in the user's personnel file. Users shall be responsible for maintaining the security of their IDs and passwords. Unique user IDs shall be individually assigned in order to maintain accountability and each ID shall be used by a single individual who is responsible for every action initiated by the account linked to that ID. Where supported, the system shall display (after successful login) the date and time of last use of the individual's account so that unauthorized use may be detected by the user.

3.1 Concurrent Connections

For those systems that enforce a maximum number of concurrent connections for an individual user ID, the maximum number of concurrent connections must not exceed two.

3.2 User IDs for non-DHHS Employees

User IDs established for non-DHHS employees (i.e., contractors) must have a specified expiration date unless a provision for a user ID without a specified expiration date is approved in writing by the Division Information Security Official (ISO) or the designated appointee. If an expiration date is not provided, a default of thirty days must be used.

Before granting such access, it must be determined that the existing access controls adequately protect the confidentiality of information contained on the system.

4.0 Logon Procedures and Controls

Divisions and Offices shall develop secure logon procedures to be applied to all network components, operating systems, applications, and databases that utilize a user ID and authentication mechanism to minimize the risk of unauthorized access. A logon message shall be displayed when users attempt to log on to IT systems which shall warn against unauthorized or unlawful use of DHHS systems. Terminology and technique suggested to implement the login message is described in the NC DHHS Security Standards, Administrative Standards - Information Security and Compliance Management Issues.

Divisions and Offices shall configure systems to limit the number of consecutive unsuccessful logon attempts to no more than three. If the number of consecutive unsuccessful log on attempts exceeds the established limit, the configuration shall either force a time delay before further logon attempts are allowed or shall disable the user account in such a way that it can only be reactivated by a system administrator.

Guidelines:

- Do not display information about the system or services until the logon process has successfully completed
- Do not validate the logon process until all logon data has been entered (halting the process as each input field is completed will provide an attacker with information to further refine the attack)
- Display only generic "logon failed" messages if the user does not complete the logon process successfully
- Do not identify in the "logon failed" message whether the user identification, password, or other information is incorrect

5.0 Securing Unattended Work Stations

Workstations shall be safeguarded from unauthorized access - especially when left unattended. Each Division and Office shall be responsible for configuring all workstations to require a password-protected screensaver after a maximum of thirty minutes of inactivity. Users shall not disable the password-protected configuration specifications established by their Division or Office.

6.0 Controlling Access to Operating System Software

Only those individuals designated as system administrators shall have access to operating system commands. System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application ports are opened in the system's firewall.

System design and configuration information shall be limited to only those individuals who require access in the performance of tasks or services essential to completing a work assignment, contract or program. A list of all administrative contacts for each system shall be maintained by the Division or Office.

Administrative access accounts must connect in a secure manner at all times. All authorized users of such accounts shall have adequate documentation and training. Administrative access account users shall use the account only for administrative duties. All other work performed shall be done via a regular user account. Use of "Power-User" type accounts should be severely limited as system configuration changes can be made under these credentials, where they would normally be disallowed.

When special access accounts are needed for internal or external audit, software development, software installation, or other defined need, they shall be authorized in advance by management and shall be:

- Created with a specific expiration date
- Removed when the work is completed

7.0 Controlling Access to System Utilities

Access to system utilities that are run with elevated privileges capable of bypassing or overriding system or application controls shall be strictly limited to users and administrators with a recurring need to run or use those utilities. Such system utilities shall be segregated from other applications and software to limit access to authorized users only.

Guidelines:

- Procedures are required for granting access for specific individuals to use powerful system utilities whether such use is temporary or not
- When access to system utilities is granted, such access will be documented and maintained
- Use of system utilities must be audited or logged
- System utilities that are not used or not needed shall be removed
- When granting authorization for an individual to use a system utility, Divisions and Offices must evaluate whether granting such access may violate segregation of duties if the utility allows bypassing or overriding of segregation controls
- If granting authorization to use a system utility could potentially violate segregation controls, the Division or Office shall enact precautions to ensure that this risk is otherwise mitigated
- Detailed auditing or two person control could provide assurance that segregation of duties is maintained

8.0 Managing Passwords

Divisions and Offices shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access DHHS information systems. The combination of a unique User ID and a strong password shall be the minimum requirement for granting access to an IT resource. Management approval shall be required for each user ID created. Divisions and Offices are responsible for establishing a process to ensure that identification credentials are canceled, revoked, or retrieved as appropriate when a user's job function or tasks change.

Information shall be maintained on all logon attempts to facilitate intrusion detection. Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long life passwords. Each Division or Office shall evaluate its business needs and the associated risks for its information systems in conjunction with identification and authentication requirements. Depending on the operating environment and associated exposures, additional or more stringent security practices may be required.

Guidelines:

- For secured access to systems and applications that require a low level of security, passwords shall have at least six characters of any sort
- For access to all systems and applications that require a high level of security, such as electronic fund transfer, tax and credit card transactions, or access to electronic protected health information (ePHI), passwords shall be at least eight characters
- To the extent possible, passwords shall be composed of a variety of letters, numbers, and symbols[1] with no spaces in between
- To the extent possible, passwords shall be random characters from the required categories of letters, numbers, and symbols
- Passwords shall not contain dictionary words, abbreviations, numbers, or characters substituted to create dictionary words (e.g., d33psl33p for deep sleep[2])
- A user is required to use different passwords for DHHS resources from passwords used for external, non-DHHS resources
- Password generators that create random passwords are allowed
- Password management application features that allow users to maintain password lists and/or automate password inputs shall be prohibited, except for simplified/single sign-on systems approved by the State Chief Information Officer (SCIO)

8.1 Password Management – Common

The following are common password management techniques that shall be implemented:

- Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members, or coworkers
- In special cases such as a problem investigation where a user must divulge a password, the user shall immediately change the password after the purpose for revealing the password has been achieved
- Allowing software to remember your password for you is not allowed
- Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media
- If stored, passwords shall be stored in encrypted format
- Individual user passwords (e.g., e-mail, Web and calendar) used to access systems and applications shall be changed at least every ninety days. Passwords shall not be reused until six (6) additional passwords have been created
- Passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established; leaving a password in a voice message is prohibited.

[1] For Resource Access Control Facility (RACF), valid symbols are @, $, #, and _, and the first character of a password must be a letter and the password must contain a number.

[2] Other examples of numbers/symbols for letters are 0 for o, $ or 5 for S, 1 for i, and 1 for l, as in capta1n k1rk or mr5pock

- Where possible and practicable, access to password protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law
- Passwords shall not be displayed in clear text during the logon process or other processes
- Where possible, applications that require clear text authentication shall be converted to equivalents that can use encryption
- Passwords shall be changed whenever there is a chance that the password or the system could be compromised

8.2 Password Management — System Administrators

The following are common password management techniques that shall be implemented for system administrators:

- All user passwords shall be required to be changed at least every ninety (90) days
- Passwords for administrative user accounts and accounts with special privileges shall be required to be changed at least every thirty (30) days
- A user account that has system level privileges or programs such as root access shall have a different password from all other accounts held by that user
- Password files shall be retrievable only by the security administrator or a designated alternate security administrator
- Vendor supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed
- The password for a shared administrative access account shall change when any individual who knows the password leaves the Division or Office that established the account or when job responsibilities change
- In situations where a system has only one administrator, Divisions and Offices shall establish a password escrow procedure so that, in the absence of the administrator, someone can gain access to the administrator account

9.0 Synchronizing System Clocks

To maintain the correct time and accuracy of audit logs created by information systems residing within DHHS networks, system clocks must be synchronized regularly across various platforms. System time clocks must be updated on a daily basis from a time source that agrees with the Coordinated Universal Time. The synchronized correct time must then be disseminated to all systems on DHHS networks.

When evaluating the accuracy of a time source, Divisions and Offices should consider the following:

- The location of the time source itself
- The availability of the time source
- The reliability of the time server to maintain accurate time received from the time source
- The latency between the time source and DHHS systems
- The reputation of the company hosting the time source

- Configuring authentication mechanisms for clock synchronization with hosts

10.0 Detecting Unauthorized Access

Divisions and Offices shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. All network components and computer systems used for DHHS operations must have the audit mechanism enabled and shall include logs to record specified audit events. Audit logs, whether on-line or stored on backup media, shall be protected so that no users, including system administrators, can alter them.

10.1 Monitoring Error Logs

Error logs generated by IT systems shall be regularly monitored and reviewed weekly for abnormalities and shall be:

- Cross-checked for known security events based on network, size, system type and physical location
- Enabled on each device or system on the network (e.g., servers, firewalls, routers, switches, cache engines, intrusion detection systems (IDS), and applications) as long as performance requirements are not affected
- Routinely checked for time and date accuracy
- Retained as required under the Division or Office records retention policy or the General Schedule for State Agency Records, Information Technology Records
- Error logs shall be checked against baselines to effectively verify variations from normal work-related activities
- The confidentiality, integrity, and availability of error logs shall be safeguarded

10.2 Monitoring Operational Logs

Divisions and Offices shall designate trained staff to review daily operational audit logs for abnormalities. Logs to be reviewed include the following:

- Network components
- Systems
- Applications
- User Event Logs

Any abnormalities and/or discrepancies between the logs and the baseline shall be reported to management. Since operational logs also provide an audit trail in the event of a security incident, the audit logs shall capture the following and contain the User ID, date and time of an event:

- System restart or shutdown
- Application start up, restart, and/or shutdown

- Application login and logout activity - both failed and successful
- Attempts to create, remove, or set passwords or change system privileges
- Unauthorized attempts to access network and system resources
- Attempts to initialize, remove, enable, or disable accounts, or services and changes to system security parameters
- Changes to the auditing function, including enabling or disabling auditing and changing events to be audited
- System errors and corrective action(s) taken
- Failed read and write operations on the system directory
- Use of system utilities and special system privileges

Personnel responsible for audit logs must ensure:

- That the Division or Office has established a current, reliable baseline that can be compared to audit logs to determine whether any abnormalities are present
- That all operational audit logs are retained in accordance with the General Schedule for State Agency Records, Information Technology Records as established by the Government Records Branch of the Department of Cultural Resources

10.3 Logging of Administrator Activity

All user ID creation, deletion, and privilege change activity performed by system administrators and others with privileged user IDs shall be logged. These logs should be reviewed daily.

10.4 Configuration of Logging and Event Recording

Where possible, all event logs shall be configured to retain records to their maximum log size allowed and to only overwrite or purge data when log size has been exceeded.

11.0 Controlling Remote User Access

Remote access to the State's network and connected elements shall be permitted through a DHHS managed secure tunnel. Access can be attained through a Virtual Private Network (VPN), Open Standard Protocol such as Secure Shell (SSH), or Internet Protocol Security (IPSec) that provides encryption and secure authentication.

11.1 Authentication

The authentication and authorization system for remote access shall be managed by the Divisions or Offices. Divisions or Offices that need centralized network infrastructure services shall use the statewide authentication and authorization service known as North Carolina Identity Management Service (NCID). Authentication for remote access shall be strong and passwords shall not traverse the network in clear text and must meet minimum requirements as documented in approved security policies and standards. Each user who remotely accesses an internal network or system shall be uniquely identifiable.

11.2 Authorization and User Access Issues

User access to DHHS information resources is accompanied by responsibilities. It is the policy of DHHS to hold users accountable for their actions. When the security of DHHS information resources is thought to be jeopardized by user activity, appropriate response is required.

11.3 User ID Use Responsibilities

All users who require remote access privileges shall be responsible for the activity performed with their user IDs. User IDs shall never be shared with those not authorized to use the ID. User IDs shall not be utilized by anyone but the individuals to whom they have been issued; users are forbidden to perform any activity with user IDs belonging to others.

11.4 Revocation/Modification

Remote access shall be revoked at any time for reasons including noncompliance with security policies, request by the user's supervisor, the Division Information Security Official (ISO), or if there is a negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated immediately upon a workforce member’s termination from service. Remote access privileges shall be reviewed upon a workforce member’s change of assignments and in conjunction with regularly scheduled security assessments.

11.5 Anonymous Interaction

With the exception of Web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any DHHS system or network anonymously (for example, by using “guest” user IDs).

11.6 Resource Access and Configuration Issues

Authorizations permit access to system resources. Additional controls are necessary to ensure that the authorization access system is not circumvented. Controls such as privilege access controls, time-out controls, remote system access controls, dial-up server controls, and remote access logging controls must all be considered as required.

11.7 Privilege Access Controls

All computers permanently or intermittently connected to external networks must operate with internal user privilege access controls approved by DHHS PSO or delegated authorities. Multi-user systems must employ user IDs unique to each user and employ user privilege restriction mechanisms, including directory and file access permissions.

11.8 Time-Out Connection Controls

Network connected single-user systems shall employ DHHS approved hardware or software mechanisms that control system booting and that include a time-out after no activity (for example, a screen saver). To the extent possible, all systems accepting remote connections from public network connected users (users connected through dial-up phone modems, dial-up Internet service providers, or broadband) shall include a time-out system. This time-out system must terminate all sessions that have had no activity for a period of no more than thirty (30) minutes. An absolute time-out shall occur after twenty-four hours of continuous connection and shall require reconnection and authentication to re-enter the DHHS network. In addition, all user IDs registered to networks or computers with external access facilities shall be automatically suspended after a period of thirty (30) days of inactivity.

11.9 Remote System Access for Systems Management Controls

Administrators shall take all precautions necessary to ensure that administrative activities performed remotely cannot be intercepted or spoofed by others.

Guidelines:

- Ensure logs include timestamps in their entries
- Follow or exceed encryption transmission standards listed herein
- Employ dial-back mechanisms as appropriate

Enhanced authentication and encryption mechanisms shall be used to protect data used for remote management of network devices or servers.

11.10 Access to Single-Host System

Remote access to single-equipment hosts (i.e., DHHS servers, Web hosting equipment) shall be permitted provided that the following requirements are met:

- Dial-up modem service: A DHHS Division or Office shall provide dial-up modem service only if that service is limited exclusively to their employees and contractors
- Web hosting servers shall provide anonymous or authenticated access to pages only if the service host prevents Onward Connection to the DHHS Network

11.11 Dial-up Server Controls

Any dial-up server that grants network access must authenticate each user, minimally, by a unique identification with password and shall encrypt the data stream. All calls must be logged, and logs of access shall be retained for ninety (90) days. At the completion of each dial-up session to a server, the accessing workstation shall be secured via password.

11.12 Remote User Logging

DHHS IT systems shall support the capability for all remote access occurrences to be logged (user ID, date/time, and duration of connection at a minimum). Audit logs of remote access activities shall be maintained for at least 90 days.

12.0 Third Party Access

Third party access to DHHS Divisions and Offices resources shall be granted on a need to use basis. Third party contracts shall specify the access, roles, and responsibilities of the third party before access is granted.

References:

- HIPAA Administration Simplification - Act 45 C.F.R. Part 160 and 164.
  - HIPAA – 45 C.F.R. § 164.308(a)(4) Information access management.
  - HIPAA – 45 C.F.R. § 164.308(a)(5)(i) Security Awareness and Training .
  - HIPAA – 45 C.F.R. § 164.308(a)(5)(ii)(C)Log-in Monitoring and (D) Password Management.
  - HIPAA – 45 C.F.R. § 164.310 (a)(1) Facility Access Controls.
  - HIPAA – 45 C.F.R. § 164.310 (2)(iii) Accountability.
  - HIPAA – 45 C.F.R. § 164.312 (a)(1) Access Control.
  - HIPAA – 45 C.F.R. § 164.312(b) Audit controls.
  - HIPAA – 45 C.F.R. § 164.312(d) Person or entity authentication.

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 2 – Controlling Access to Information and Systems, Section 01: Controlling Access to Information and Systems
    - Section 020102 - Managing User Access
    - Section 020103 - Securing Unattended Work Stations
    - Section 020105 - Controlling Access to Operating System Software
    - Section 020106 - Managing Passwords
    - Section 020108 - Restricting Access
    - Section 020112 - Controlling Remote User Access
    - Section 020113 - Types of Access Granted to Third Parties
    - Section 020114 - Why Access is Granted to Third Parties

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 3 - Processing Information and Documents, Section 01: Networks
    - Standard 030103- Accessing Your Network Remotely
  - Chapter 3 - Processing Information and Documents, Section 02: Systems Operation and Administration
    - Standard 030204 - Permitting Third-Party Access
    - Standard 030208 - Monitoring Error Logs
    - Standard 030211 - Monitoring Operational Audit Logs

        - Standard 030212 Synchronizing System Clocks
        - Standard 030217 - Log-On Procedures
        - Standard 030218 - Systems Utilities
        - Standard 030219 - System Use Procedure.

- NC Statewide Information Security Manual, Version No. 1
    - Chapter 10 - Addressing Personnel Issues Relating to Security, Section 03: Personnel Information Security Responsibilities
        - Standard 100302 - Keeping Passwords/PIN Numbers Confidential

- NC DHHS Security Standards
    - Administrative Security Standard
        - Information Security and Compliance Management Issues Standard

- NC DHHS Security Standards
    - Application Security Standard
        - Application Security Controls Standard
        - Data Management and Storage Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
    - Information Systems Review and Auditing Policy
    - Security Testing Policy
    - IT Operations Security Policy
    - User Authorization, Identification and Authentication Policy
    - Data Protection Policy